REMARKS

This Amendment and Response to Non-Final Office Action is being submitted in response to the non-final Office Action mailed July 1, 2008. Claims 1-21 are pending in the Application.

Claims 1-12, 15-16, and 19-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* (U.S. Pat. Pub. 20030186679) in view of Zuk *et al.* (U.S. Pat. Pub. 20030154399) and Campbell *et al.* (U.S. Pat. No. 6,893,850).

Claims 13-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.* as applied to Claim 1, and further in view of Won *et al.* (U.S. Pat. No. 6,754,488).

Claims 17-18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.*as applied to Claim 1, and further in view of Ammon *et al.* (U.S. Pat. Pub. No. 2003017289).

In response to these rejections, Claims 1, 19, and 21 have been amended to further clarify the subject matter which Applicant regards as the invention, without prejudice or disclaimer to continued examination on the merits. These amendments are fully supported in the Specification, Drawings, and Claims of the Application and no new matter has been added. Based upon the amendments and the arguments presented herein, reconsideration of the Application is respectfully requested.

Examiner's Response to Arguments

Examiner argues that Zuk *et al.*, at the very least implicitly, discloses wireless policy as argued and included in the previously presented amendments. (Non-Final OA, page 2). Applicants respectfully submit that Examiner is misreading this portion of Zuk *et al.* Zuk *et al.* teach a wireless network (element #70), however Zuk *et al.*'s MMIDP system does not deal with the wireless network. Rather, Zuk *et al.* inspect wired packets from a base station 72 (FIG. 3). Zuk *et al.* are not teaching wireless policy as recited in the claims -

wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings. Instead, Zuk *et al.* do not see the packets until they reach the wired network (Note, in all the FIGS. in Zuk *et al.*, the MMIDP sensors are inspecting packets on the wired network, not the wireless network). Accordingly, it is not possible for Zuk *et al.* to teach wireless policy since the system taught by Zuk *et al.* only sees packets after they enter the wired network from the base station 72. After entering the wired network, packets lose their wireless specific settings.

Next Examiner argues that Zuk *et al.* teach security technologies which maintain privacy through authentication and encryption (¶¶[0005]-[0008]). Again, the remarks presented above apply here as well. These sections in Zuk *et al.* discuss VPNs, firewalls, anti-virus, password protection, etc. These are not relevant to wireless policy as claimed by Applicants. Rather, these techniques are discussing wired intrusion detection systems which are not the same as wireless-based systems. Zuk *et al.* fail to disclose, teach, or suggest wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings. Additionally, Challener *et al.* and Campbell *et al.* fail to teach or suggest these limitations as well.

Zuk *et al.* also fails to disclose, teach, or suggest wireless statistics. Examiner is arguing that wired statistics are the same thing, such as top IP address used in attacks, the top attacks, the number of alarms and incidents generated, whether the alarm is real or false, etc. Applicants' wireless statistics not only include the alarms, but also are used to generate alarms through various wireless-related thresholds. Through these wireless statistics, Applicants are able to detect anomalous behavior and identify a rogue wireless device or an allowed wireless device which is acting improperly. Applicants respectfully disagree with Examiner that the same techniques in wired intrusion detection systems would apply to wireless.

Also, Examiner argues that Zuk *et al.* teaches wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based

tests. Again, the remarks above apply with equal force here. It is not possible for Zuk *et al.* to teach these tests since Zuk *et al.* views packets after they leave the base station 70. Further, Challener *et al.* fails to cure these deficiencies. Challener *et al.* teach monitoring the signal strength with a workstation of rogue APs. It does not teach or suggest stripping header information off wireless packets for gather statistics and for performing these tests. It is not possible to combine Challener *et al.* and Zuk *et al.* since Zuk *et al.* monitor packets only on a wired portion of the network (i.e., without corresponding wireless header information) and Challener *et al.* do not teach storing and processing wireless header information.

Additionally, Examiner contends that Zuk *et al.* teach detecting anomalous behavior. Respectfully, this is not detecting attacks as argued by examiner. As discussed herein, it is not possible for the combination of Challener *et al.* and Zuk *et al.* to detect authorized wireless devices which are displaying anomalous behavior because neither teaches gathering wireless statistics (Zuk *et al.* cannot because the wireless header is removed once on the wired network).

Applicants respectfully note that Challener *et al.* only monitor two data points: whether there is a rogue AP and the signal strength of the rogue AP (¶[0026]). There is no collection of wireless statistics to detect unauthorized devices or anomalous behavior in authorized devices. Zuk *et al.* cannot cure these deficiencies since they only deal with wired portions of the network. It is not sufficient to say that there is an attached wireless network in Zuk *et al.* and therefore they teach Applicants' invention.

Claims 1-12, 15-16, and 19-21 - §103(a) Rejection – Challener *et al.*, Zuk *et al.*, Campbell *et al.*

Claims 1-12, 15-16, and 19-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* (U.S. Pat. Pub. 20030186679) in view of Zuk *et al.* (U.S. Pat. Pub. 20030154399) and Campbell *et al.* (U.S. Pat. No. 6,893,850).

In addition to the remarks present herein, Applicants respectfully submit that none of these references teaches or suggests one or more wireless sensors.

Claim 1 has been amended to include the following new structural limitations:

a set of one or more wireless receivers on one or more wireless sensors;

a system processor in communication with the system data store and the one or more wireless sensors, wherein the system processor comprises one or more processing elements programmed or adapted to perform the steps comprising of:

Claim 19 has been amended to include the following new structural limitations:

(d) receiving data from one or more wireless sensors

Claim 20 has been amended to include the following new structural limitations:

One or more computer readable media storing instruction that upon execution by a system processor cause the system processor to perform the method of claim 19; wherein the system processor comprises a distributed processor distributed between the one or more wireless sensors and a host system.

Finally, Claim 21 has been amended to include the following new structural limitations:

one or more wireless sensors for scanning wireless traffic;

distributed rogue detection means for detecting a wireless device based upon one or more dynamic operational and security assessments operable to detect the wireless device based on behavior, wherein the assessments are performed on the received scan data, and for storing an indicator of the detected wireless device, wherein the distributed rogue detection means is distributed between the one or more wireless sensors and a host system

With regard to Claims 20 and 21, Applicants additionally note that none of the references disclose, teach, or suggest a distributed processor between the sensors and a host system for detection.

Accordingly, Applicants respectfully request withdrawal of this rejection responsive to the amendments and remarks presented herein.

Claims 13-14 - §103(a) Rejection – Challener *et al.*, Zuk *et al.*, Campbell *et al.* and Won *et al.*

Claims 13-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.* as applied to Claim 1, and further in view of Won *et al.* (U.S. Pat. No. 6,754,488). The amendments and remarks with regard to Claim 1 apply with equal force here. Therefore, Applicant respectfully requests withdrawal of this rejection.

Claims 17-18 - §103(a) Rejection – Challener *et al.*, Zuk *et al.*, Campbell *et al.*, and Ammon *et al.*

Claims 17-18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.*as applied to Claim 1, and further in view of Ammon *et al.* (U.S. Pat. Pub. No. 2003017289). The amendments and remarks with regard to Claim 1 apply with equal force here. Therefore, Applicant respectfully requests withdrawal of this rejection.

CONCLUSION

Applicant would like to thank Examiner for the attention and consideration accorded the present Application. Should Examiner determine that any further action is necessary to place the Application in condition for allowance, Examiner is encouraged to contact undersigned Counsel at the telephone number, facsimile number, address, or email address provided below. It is not believed that any fees for additional claims, extensions of time, or the like are required beyond those that may otherwise be indicated in the documents accompanying this paper. However, if such additional fees are required, Examiner is encouraged to notify undersigned Counsel at Examiner's earliest convenience.

Respectfully submitted,

Date: September 17, 2008

/ Lawrence A. Baratta Jr./
Lawrence A. Baratta Jr.
Registration No.: 59,553

Christopher L. Bernard
Registration No.: 48,234

Attorneys for Applicants

Clements | Bernard | Miller
1901 Roxborough Road, Suite 300
Charlotte, North Carolina 28211 USA
Telephone: 704.366.6642
Facsimile: 704.366.9744
lbaratta@worldpatents.com